

# BEST AVAILABLE COPY

(19)



JAPANESE PATENT OFFICE

## PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2002023627 A

(43) Date of publication of application: 23.01.02

(51) Int. Cl

G09C 1/00  
G06F 17/60

(21) Application number: 2000200557

(22) Date of filing: 03.07.00

(71) Applicant: NIPPON TELEGR & TELEPH CORP <NTT>

(72) Inventor: HASHIMOTO SHOICHI  
MASAMOTO HIROSHI

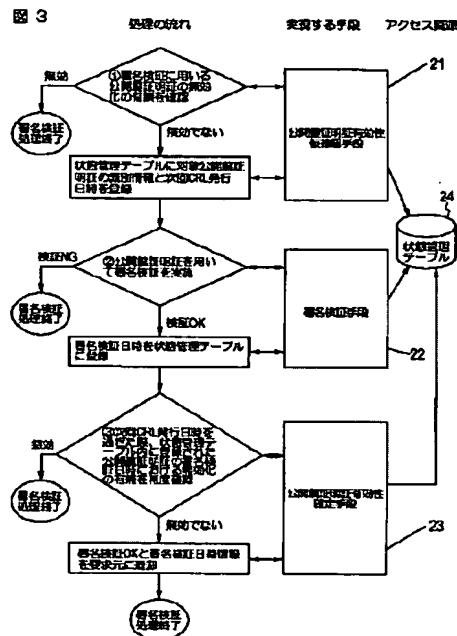
### (54) DEVICE AND METHOD FOR VERIFYING SIGNATURE

#### (57) Abstract:

**PROBLEM TO BE SOLVED:** To confirm that a public key certificate used for the verification is surely not invalid at the time of verifying a signature.

**SOLUTION:** This device (1) confirms that the public key certificate to be used for verifying a signature is not invalidated; (2) verifies the signature by using the public key, and registers the public key certificate identification information, the date of issue of the next CRL (invalidated public key certificate list), and the date of the signature verification in a state management table according to each processing number; and (3) when the next CRL issue date has passed, the device confirms that each certificate identification information was not invalidated on the date when each information was used for the signature verification.

COPYRIGHT: (C)2002,JPO



**ONE PAGE BLANK (USPTO)**

(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-23627

(P2002-23627A)

(43)公開日 平成14年1月23日 (2002.1.23)

(51)Int.Cl.<sup>7</sup>

G 0 9 C 1/00

識別記号

6 4 0

F I

G 0 9 C 1/00

テーマコード<sup>\*</sup>(参考)

6 4 0 B 5 B 0 4 9

6 4 0 Z 5 J 1 0 4

G 0 6 F 17/60

1 4 0

G 0 6 F 17/60

1 4 0

5 1 2

5 1 2

審査請求 有 請求項の数 2 O L (全 9 頁)

(21)出願番号

特願2000-200557(P2000-200557)

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(22)出願日

平成12年7月3日(2000.7.3)

(72)発明者 横本 正一

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

(72)発明者 政本 廣志

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

(74)代理人 100066153

弁理士 草野 韶 (外1名)

最終頁に続く

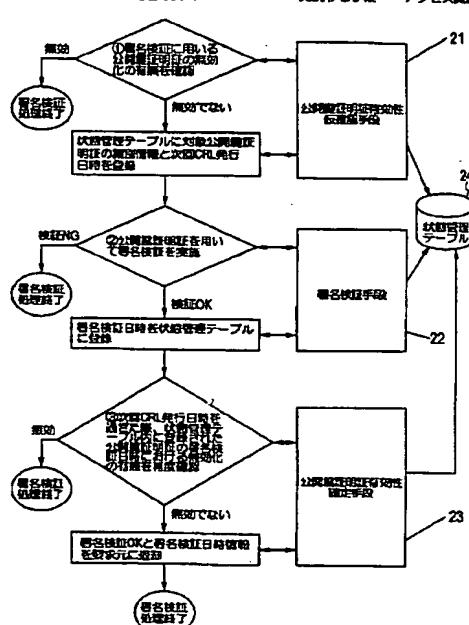
(54)【発明の名称】署名検証装置及び署名検証方法

(57)【要約】

【課題】署名検証した時点でその検証に用いた公開鍵証明証が確かに無効とされてないものであることを確認可能とする。

【解決手段】①署名検証に用いる公開鍵証明証が無効化されていないことを確認し、②その公開鍵を用いて署名検証を行い、その公開鍵証明証識別情報、次回CRL(無効公開鍵証明証リスト)発行日時、署名検証日時を状態管理テーブル24に各処理番号ごとに登録し、③次回CRL発行日時が過ぎると、状態管理テーブル24内の各証明証識別情報について、それがその署名検証に用いた日時に無効でなかったことを確認し、そのことを検証要求元へ通知する。

図3 处理の流れ 実現する手段 アクセス箇所



## 【特許請求の範囲】

【請求項1】 处理識別子ごとに署名検証日時、公開鍵証明証識別情報、次回CRL（無効化公開鍵証明証リスト）発行日が記憶される状態管理テーブルと、  
公開鍵証明証を用いて入力された情報について署名検証  
処理を行い、上記状態管理テーブルに署名検証を行った  
日時を登録する署名検証手段と、  
署名検証処理時に、これに用いる公開鍵証明証の無効化  
の有無を確認し、上記状態管理テーブルに確認対象の公  
開鍵証明証の識別情報と次回CRL発行日時を登録する  
公開鍵証明証有効性仮確認手段と、  
次回CRL発行日時が過ぎると、上記状態管理テーブル  
内に登録された識別情報に対応する公開鍵証明証による  
署名検証日時の時点におけるその公開鍵証明証の無効化  
の有無を確認する公開鍵証明証有効性確定手段と、を具  
備することを特徴とする署名検証装置。

【請求項2】 署名検証要求を受け付けると、公開鍵証  
明証有効性仮確認手段を用いて、署名検証に用いる公開  
鍵証明証の無効化の有無を確認し、  
無効化されていない場合に、対象公開鍵証明証の識別情  
報と次回CRL発行日時を状態管理テーブルに記憶登録  
し、  
続いて上記署名検証要求された情報について上記公開鍵  
証明証を用いる署名検証処理を行い、  
その検証に合格すると、上記状態管理テーブルに署名検  
証日時を記憶登録し、  
現時刻が次回CRL発行日時を過ぎると、上記状態管理  
テーブル内の情報を読み出し、登録された識別情報に対  
応する公開鍵証明証が、その署名検証日時の時点で無効  
化されていなかったか否かを確認し、無効化されていな  
かったことが確認されると、署名検証合格とともに署名  
検証日時情報を上記署名検証要求元に通知することを特  
徴とする署名検証方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、電子データの正  
当性を確認する際に行う電子署名を検証するための装置  
及びその方法に関するものである。

## 【0002】

【従来の技術】公開鍵暗号を用いた電子署名技術によ  
り、利用者の本人確認や通信路における改竄（かいざ  
ん）の有無の確認を行うシステムでは、CA（Certific  
ation Authority：認証局）が発行する公開鍵証明証を用  
いて、電子署名の検証が行われる。公開鍵証明証には、  
信頼性を低下させないために、利用可能な有効期間が定  
められているが、公開鍵に対応する秘密鍵の漏洩や、所  
有者の身元情報に変更が生じるなどの理由により、有効  
期間内であってもCAが残りの有効期間内の効力を強制  
的に無効化する場合がある。このため、電子署名を検証  
する際には、公開鍵証明証がCAによって無効化されて

いないことを確認してその公開鍵を利用する必要があ  
る。一般にCAは、利用者からの公開鍵証明証の無効化  
依頼を受け付けると、CRL（Certificate Revocation  
List：証明書取消リスト）と呼ばれる無効化された公開  
鍵証明証識別情報の一覧を定期的に発行して、外部の利  
用者に無効化された公開鍵証明証の情報を周知させる。  
そこで図8に示すように署名検証装置11ではCA12  
から定期的に発行されるCRLをCRL取得手段13に  
より取得してCRL記憶部14に記憶しておく。署名檢  
証処理部15で署名検証を行う場合はまずCRL検索手  
段16により、その検証に用いる公開鍵証明証識別情報  
が、CRLリストにあるかをCRL記憶部14を検索  
し、CRLリストにないことつまり対象公開鍵証明証が  
無効化されていないことを確認して、その公開鍵を用い  
て、署名検証処理を行う。

【0003】また、このCRLをCAから取得し、公開  
鍵証明証の無効化の有無の確認を代行する機関であるVA  
（Validation Authority：検証局）を設けて、ここへ  
の問い合わせにより、対象公開鍵証明証が無効化されて  
いないことを確認する方法もある。つまり図9に示すよ  
うに、検証局18ではCAから定期的に発行されるCRL  
を取得記憶しておき、署名検証装置11で署名検証を行  
う場合、まずVA問い合わせ手段19により対象公開  
鍵証明証の識別情報を検証局18へ送り、その証明証が  
有効か否かの問い合わせを行い、検証局18はその証明  
証識別情報により、CRL記憶部を検索して、なければ  
有効であること、あれば無効であることを問い合わせの  
あった署名検証装置11へ返送する。署名検証装置11  
は有効の回答があると、その公開鍵証明証の公開鍵を用  
いて検証処理を行う。

## 【0004】

【発明が解決しようとする課題】上記に示したCRL  
は、CAによって定期的に発行されるため、一度最新の  
CRLが発行されると、その発行の後でCAに無効化申  
請された公開鍵証明証の識別情報は、次回に発行される  
CRLに掲載されることになり、それが発行されるま  
で、CA外部の利用者は無効化された公開鍵証明証の最  
新情報を知ることができない。したがって、署名検証に  
用いる公開鍵証明証の無効化の有無をCRLを用いて確  
認する場合、署名検証時において最新のCRLに確認対  
象の公開鍵証明証の情報が掲載されていないことを確認  
できたとしても、その最新のCRLが発行されてから署  
名検証を行うまでの間に、対象公開鍵証明証が無効化さ  
れている可能性があり、署名検証を行った日時におい  
て、確かに署名検証に用いた公開鍵証明証が無効化され  
ていないことを保証することができないという課題があ  
った。

【0005】上記の課題を図10を用いて説明する。CA  
により時刻T1にCRLが発行され、次回CRL発行  
日時がT5である状況を想定する。この状況において、

時刻T2で利用者AがCAに対して公開鍵証明証の無効化申請を行い、その後、時刻T3に利用者Aから例えばシステムBに対してサービス申請が行われ、システムBの署名検証装置において時刻T4に利用者Aの署名検証が行われたとする。その際、システムBの署名検証装置は署名検証に用いる公開鍵証明証が無効化されていないことを、時刻T1に発行されたCRLを用いて確認するが、このCRLでは、時刻T1以前に受け付けられた無効化証明証しか確認できず、時刻T2に無効化された公開鍵証明証の識別情報を確認することができないため、それを有効な公開鍵証明証であるとして署名検証を行い、その検証に合格すると、システムBが利用者Aにサービスを提供することになる。しかしながら、時刻T5に発行される新たなCRLには、時刻T2で利用者Aの公開鍵証明証が無効化されたことの情報が掲載されるため、時刻T4で行った署名検証は正しい処理でないことになる。

[0006]

【課題を解決するための手段】上記に示した課題を解決するため、この発明では、署名検証を行う際に、これに用いる公開鍵証明証の無効化の有無を、次回のC R L 発行日時以降に再度確認することにより、署名検証を行った日時において、確かに署名検証に用いた公開鍵証明証が無効化されていなかったことを保証する。まず図1に、この発明の機能構成を示し、構成要素である各手段を以下に説明する。

#### · 公開鍵證明証有効性仮確認手段 2.1

署名検証処理時において、これに用いる公開鍵証明証の無効化の有無を確認し、無効化されていないことが確認された場合、状態管理テーブル 2-4 にその公開鍵証明証の識別情報と、次回の CRL 発行日時をその処理識別子と共に登録する。

・署名検証手段22

公開鍵証明書を用いて依頼された署名検証処理を行い、署名検証がOK（合格）であった場合に、状態管理テーブル2-4に署名検証を行った日時を登録する。

#### • 公開鍵證明証有效性確定手段 2 3

状態管理テーブル24内に登録された公開鍵証明証の識別情報について、登録された次回CRL発行日時以降に、その識別情報に対応する公開鍵証明証の署名検証日時の時点における、その公開鍵証明証の無効化の有無を確認し、最終的な署名検証結果を返却する。

#### ・状態管理テーブル 2 4

署名検証を行った日時における、その検証に用いた公開鍵証明証の無効化の有無が確認可能となるまでの間、例えば図2に示すように署名検証処理ごとにその識別子を付け、その処理識別子と、その署名検証日時や、署名検証に用いた公開鍵証明証の識別情報、次回CRL発行日時などの署名検証処理の状態を記憶して管理するテーブルである。

- 更に時計25を備え状態管理テーブル24に対する読み書き消去は読み書き制御部26により行う

〔0007〕次に、上記の各構成要素を用いた署名検証方法の流れを、図3を用いて説明する。

- ①例えばサービスを提供するシステム中のあるモジュールからの署名検証要求を受け付けると、公開鍵証明証有効性仮確認手段2.1を用いて、署名検証に用いる公開鍵証明証が、既にCAによって無効化されていないことを確認し、無効化されていない場合、状態管理テーブル2.4に対象公開鍵証明証の識別情報と、次回CRL発行日時を登録する。すでに無効化されていることが確認された場合には、これを、署名検証要求元（この例ではシステムの前記モジュール）に通知して処理を終了する。

②①で署名検証に用いる公開鍵証明証の無効化が確認されなかれば、署名検証手段③に上れる。

- いなかった場合、署名検証手段ごとにより、システムのモジュールから依頼された署名検証処理を公開鍵証明書を用いて行い、検証OK（合格）であった場合、状態管理テーブル24に署名検証を行った日時を登録する。また、検証NG（不合格）であった場合には、これを署名検証要求元（前記モジュール）に通知して処理を終了する。

③状態管理テーブル2.4に登録した次回CBI発行日時

- をシステム時刻(現在時刻)が過ぎた際に、公開鍵証明証有効性確定手段23を用いて、状態管理テーブル24内のその次回CRL発行日時が登録されている識別情報に対応する公開鍵証明証が、署名検証日時の時点で無効化されていなかったことを確認する。ここで、再度無効化されていないことが確認された場合、検証OKとともに状態管理テーブル24に登録された署名検証日時情報を

無効化されていた場合には、検証NGを呼び出し元に通知して処理を終了する。

- 〔0008〕以上に示した処理方法を用いることにより、署名検証要求があった時に、その公開鍵証明証が無効化されていればそのことを署名検証要求元に直ちに通知することができ、また無効化されていないことにより、署名検証を行いそれが不合格の場合も、このことが直ちに通知される。更に署名検証処理を行った日時において、署名検証に用いた公開鍵証明証が確かに無効化さ

れていたことを保証することが可能となる。また署名検証要求があった後、次のCRLの発行を待って、その公開鍵証明証が無効化されていないことを確認して署名検証することも考えられるが、その前のCRLで既に無効化されている場合や、署名検証に不合格となる場合に、これらの通知が遅れるが、この発明ではそのようなことがない。

(0009)

【発明の実施の形態】この発明の実施例を図4乃至図7を用いて説明する。この実施例では、図4に示すようにCAが新しいC.R.I.を毎日0時に発行する状況を想

定する。システムの署名検証装置が、利用者による公開鍵証明証の無効化依頼をCAに対し行う前に署名検証を行った場合（署名検証処理（1））と、無効化依頼後に署名検証を行った場合（署名検証処理（2））の両方において、この発明による署名検証処理の様子を、図5及び図6を用いて説明する。

【0010】まず、2000/5/15の0時にCAから新たなCRLが発行された後、システムBが10時に利用者Aからの署名検証を伴うサービス申請（1）を受け付けたところを想定する。

S1. サービス申請（1）の受付処理に基づきそのモジュールから、署名検証装置の公開鍵証明証有効性仮確認手段21が署名検証処理（1）の要求を受け付けると、まず、公開鍵証明証無効化確認機能を用いて、署名検証に用いる公開鍵証明証の無効化の有無を確認する。この時点では利用者Aは無効化申請を行っていないため、利用者Aの公開鍵証明証の無効化は確認されない。公開鍵証明証無効化確認機能は、自らがCRLをCAから取得してCRLの中身を確認する方法や、VAへの問い合わせにより確認する方法が既に知られており、これらを利用することにより実現可能である。なお公開鍵証明証は利用者Aがサービス申請時に送る場合、あるいはシステムBが予めもっている場合などがあり、署名検証装置にはシステムBから供給される。

【0011】S2. S1の確認で無効化が確認されなかった場合、処理識別子、確認対象の公開鍵証明証の識別情報、次回CRL発行日時情報を、テーブル登録機能を用いて状態管理テーブル24に登録する。ここでは、図7に示すように処理識別子が「処理（1）」であり、確認対象の公開鍵証明証は、発行者名が「CA-1」、所有者名が「利用者A」、通し番号が「1001」の公開鍵証明証であったこととしてこれらを登録するとともに、次回CRL発行日時情報である「2000/5/16 0:00:00」も状態管理テーブル24に登録する。テーブル登録機能は、例えば市販のDBシステムにおいてDBの情報を書き換えるためのDB登録機能などが利用可能である。次回CRL発行日時情報はCRL内にその情報が記載されておりこれを参照するか、VAからの問い合わせ結果に一般に含まれており、その参照等により取得する。

【0012】S3. 次に、署名検証手段22は、公開鍵証明証内から公開鍵を取り出し署名検証を行う。署名検証機能は、公開鍵、検証対象である電子署名、署名の生成対象である電子データを入力として電子署名の正当性の確認を行う機能であり、既存の暗号技術を用いて容易に実現可能である。

S4. S3の署名検証がOKであった場合、テーブル登録機能を用いて、署名検証日時情報を状態管理テーブル24に登録する。ここでは、署名検証日時が「2000/5/15 10:00:10」であったこととして、

これを図7に示すように処理（1）に対し登録する。なお署名検証が不合格であった場合は、そのことが署名検証要求元モジュールに直ちに通知され、また状態管理テーブル24中の対応する処理識別子「処理（1）」の欄が消去される。

【0013】ここで、サービス申請（1）の後で、利用者Aによる公開鍵証明証の無効化申請がCAに対して行われ、その後、再度、利用者Aからのサービス申請（2）を受け付けたところを次に想定する。

10 S5. サービス申請（2）の受付処理に基づき、署名検証装置の公開鍵証明証有効性仮確認手段21が署名検証処理（2）の要求を受け付けると、S1と同様に、公開鍵証明証無効化確認機能を用いて、署名検証に用いる公開鍵証明証の無効化の有無を、最新のCRLにより確認する。この時点で利用者Aは既に無効化申請を行った後であるが、この時点でCRLには、その情報はまだ掲載されていないため、システムBの署名検証装置では、利用者Aの公開鍵証明証の無効化は確認されない。

【0014】S6. S5の確認で無効化が確認されなかっ

たため、処理識別子、確認対象の公開鍵証明証の識別情報、次回CRL発行日時情報を、テーブル登録機能を用いて状態管理テーブル24に登録する。ここでは、図7に示すように処理識別子が「処理（2）」であり、確認対象の公開鍵証明証はS2のときと同様であったとし、次回CRL発行日時情報である「2000/5/16 0:00:00」とともに状態管理テーブル24に登録する。

【0015】S7. 次に、署名検証手段22は、公開鍵証明証内から公開鍵を取り出し署名検証を行う。

30 S8. S7の署名検証がOKであった場合、テーブル登録機能を用いて、署名検証日時情報を状態管理テーブル24に登録する。ここでは、署名検証日時が「2000/5/15 13:00:10」であったとして、これを図7に示すように処理（2）に対して登録する。

【0016】続いて、図6に示すように次回CRL更新日時である2000/5/16 0時を過ぎ、CAから新たなCRLが発行されたところを想定する。

S9. 公開鍵証明証有効性確定手段23は時計25の現在時刻と状態管理テーブル24内に登録済の次回CRL発行日時とを比較し、現在時刻が次回CRL発行日時を過ぎ、その新しいCRLによる確認が可能な状態になると、状態管理テーブル24に登録された各処理識別子に対応する情報の内、状態管理テーブル24内に登録された次回CRL発行日時が、システム時刻（現在時刻）より前の処理識別子の存在をテーブル参照機能により確認し、これら処理識別子のそれぞれについて、署名検証日時における公開鍵証明証の無効化の有無を、公開鍵証明証無効化確認機能を用いて確認する。つまりこの時点で最新のCRLには、「2000/5/15 11:00:00」に利用者Aの公開鍵証明証（発行者名が「C

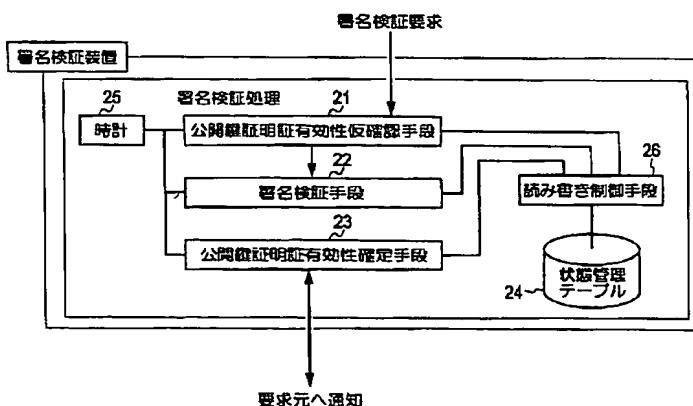
A-1」、所有者名が「利用者A」、通し番号が「1001」)が無効化されていることの情報が掲載されているため、これにより図7に示した例では「処理(1)」の処理については、署名検証日時である「2000/5/15 10:00:10」の時点が無効化申請時刻より前であるから利用者Aの公開鍵証明証は無効化されていなかったことが確認され、「処理(2)」の処理については、署名検証日時である「2000/5/15 13:00:10」の時点が無効化申請時刻より後であるから利用者Aの公開鍵証明証は無効化されていたことが確認される。ここで利用されるテーブル参照機能は、例えば市販のDBシステムにおいてDBの情報を参照するためのDB参照機能などが利用可能である。

【0017】S10. 戻り値返却機能を用いて、署名検証要求モジュールにサービス申請(1)の処理については「署名検証OK」と「署名検証日時 2000/5/15 10:00:10」を返却し、サービス申請(2)の処理については、「署名検証NG」を返却した後、テーブル削除機能を用いて、状態管理テーブル24内の該当処理の情報を削除する。戻り値返却機能は、通常のプログラム作成において利用可能な機能であり、テーブル削除機能は、例えば市販のDBシステムにおいてDBの情報を削除するためのDB削除機能などが利用可能である。

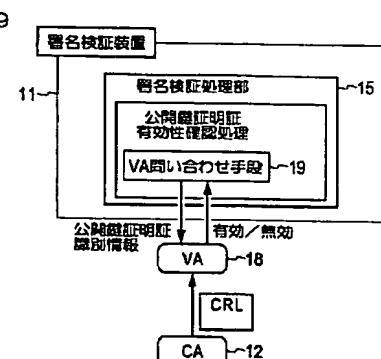
〔0018〕上記のように、署名検証装置が署名検証を行う際、これに用いる公開鍵証明証の無効化の有無を、署名検証日時の時点における無効化の有無が確認可能となる次回CRL発行日時以降に再度確認することにより、署名検証日時において確かに署名検証に用いた公開鍵証明証が無効化されていなかったことを保証した、正当な署名検証を行うことが可能となる。また署名検証要求を受けた際に、CRLによる公開鍵証明証の無効化の\*

[圖 1]

1



[圖 9-1]



(6)

特開2002-23627

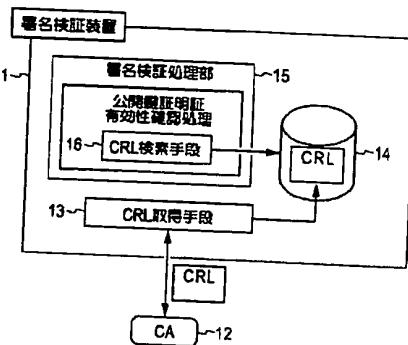
【図2】

図2

処理識別子	署名検証日時	公開鍵証明書識別情報	次回CRL発行日時
処理番号1	2000/05/15 10時20分00秒	公開鍵証明書1	2000/05/16 00時00分00秒
処理番号2	2000/05/15 13時00分00秒	公開鍵証明書2	2000/05/16 00時00分00秒
処理番号3	2000/05/15 20時00分00秒	公開鍵証明書3	2000/05/16 00時00分00秒

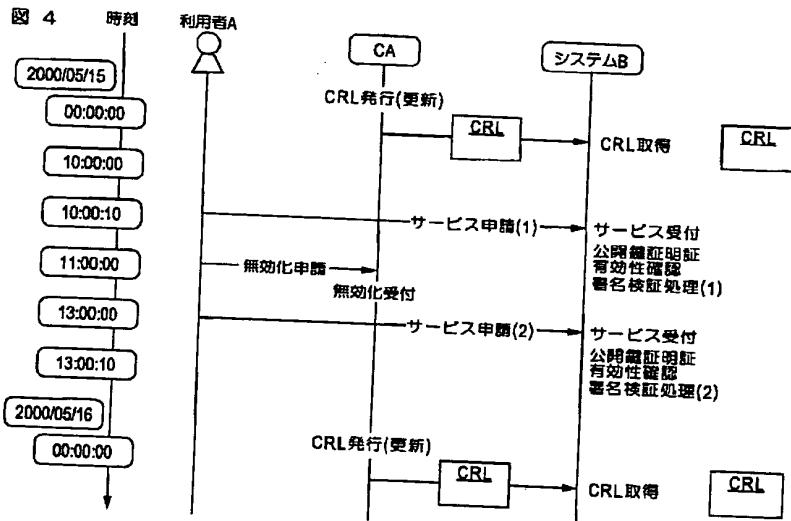
【図8】

図8



【図4】

図4 時刻

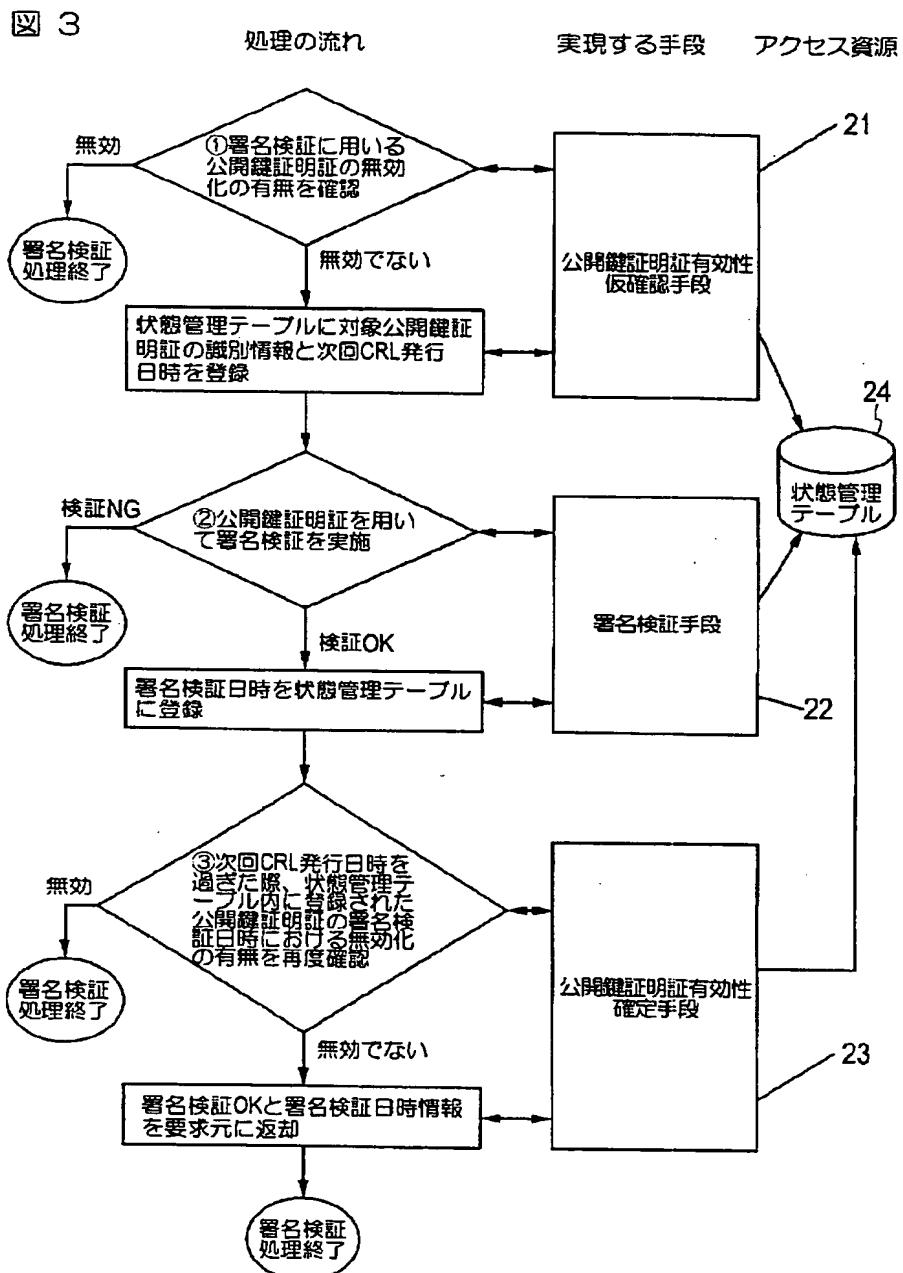


【図7】

図7

処理識別子	署名検証日時	公開鍵証明書識別情報			次回CRL発行日時
		発行者名	所有者名	シリアル番号	
処理(1)	2000/05/15 10:00:10	CA-1	所有者A	1001	2000/05/16 0:00:00
処理(2)	2000/05/15 13:00:10	CA-1	所有者A	1001	2000/05/16 0:00:00

【図3】



【図5】

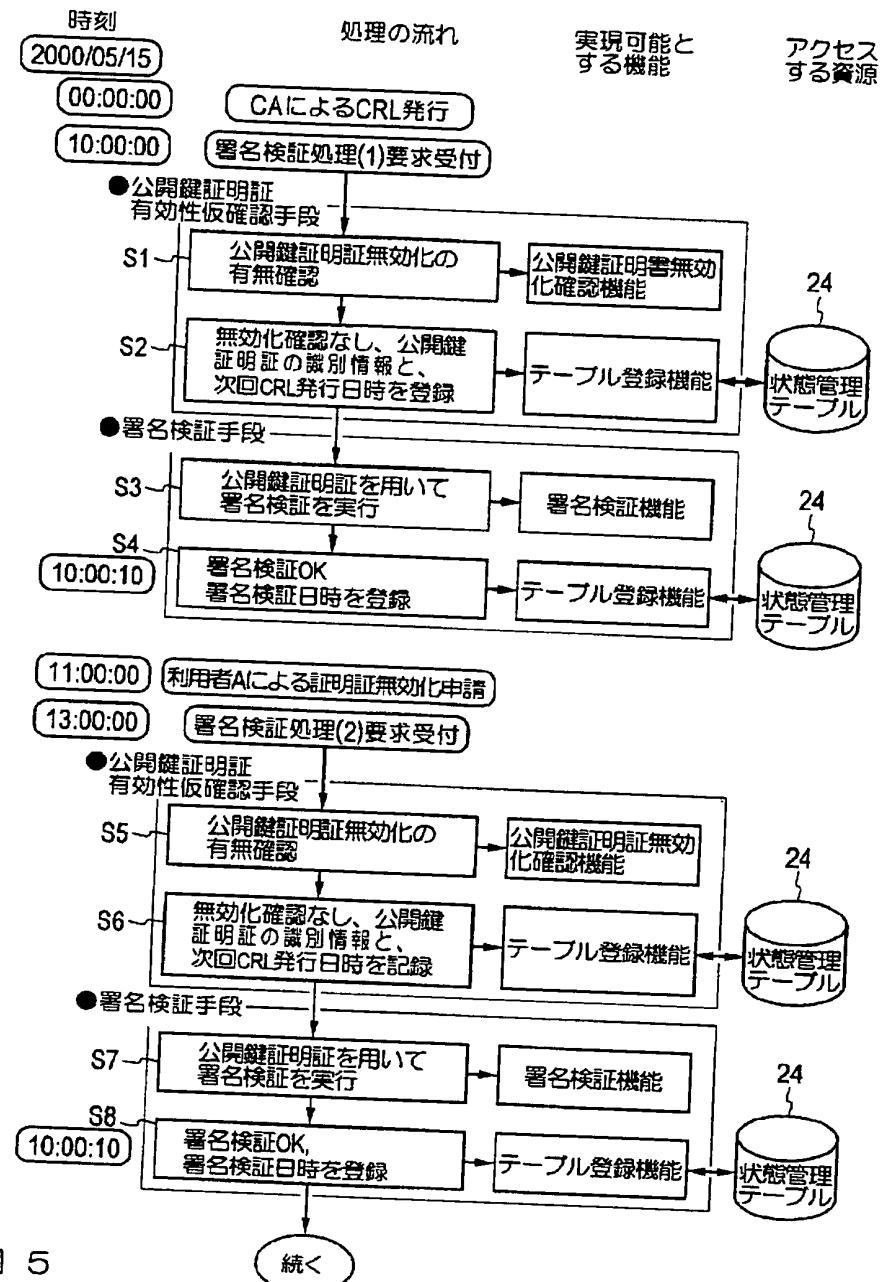


図 5

【図6】

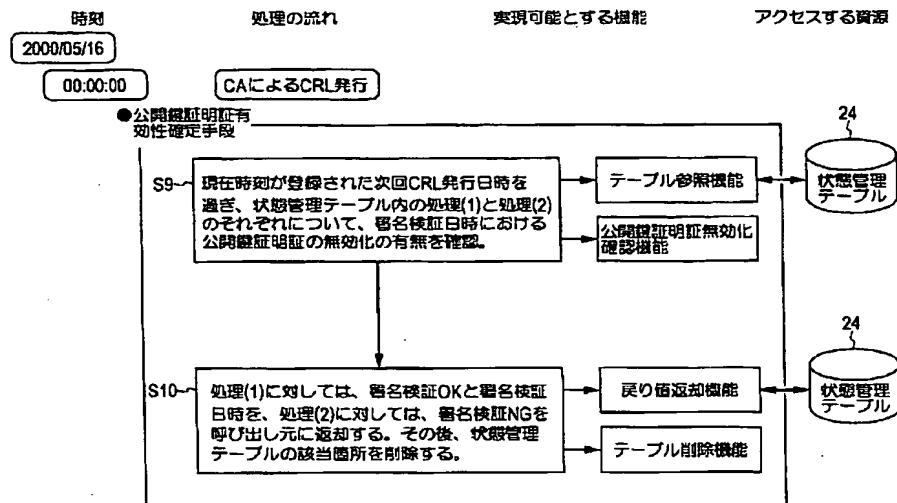
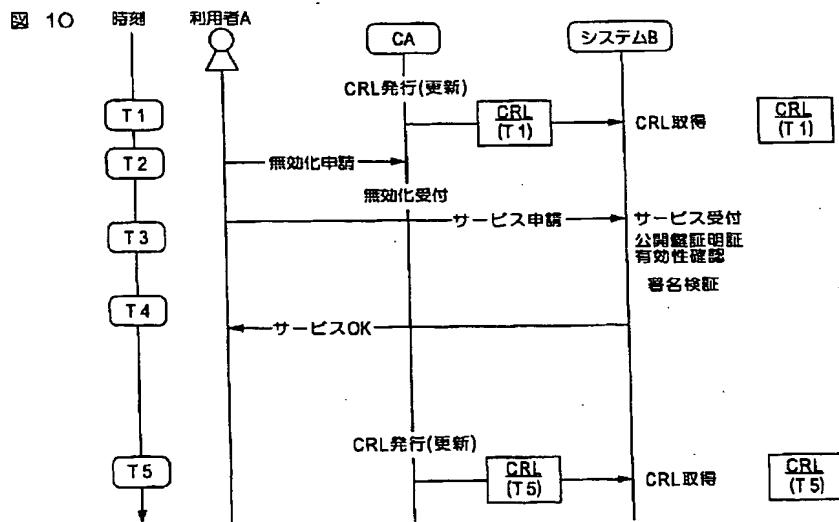


図6

【図10】



フロントページの続き

F ターム(参考) 5B049 AA05 CC31 DD05 EE05 EE09

FF09 GG10

5J104 AA09 AA16 EA05 LA03 LA06

NA02 PA07

THIS PAGE BLANK (uspro).

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

THIS PAGE BLANK (USPTO)